IN THE CLAIMS

Amended claims follow:

1. (Currently Amended) A method for establishing a cryptographic key for use between a first node and a second node using a super node, wherein the first node and the second node are energy-limited and the super node has abundant energy, the method comprising:

sending a first message from the first node to the super node, ~~wherein~~ the first message includesing a first partial key value encrypted using a public key belonging to the super node, ~~whereby~~the encrypting with the public key requiresing less energy than decrypting with a private key corresponding to the public key;

recovering the first partial key value at the super node by decrypting using the private key;

securely communicating the first partial key value to the second node; ~~and~~

establishing the cryptographic key at the second node using the first partial key value and a second partial key value created by the second node; and

utilizing a combination of public key cryptography and symmetric key cryptography with symmetric key encryption being used in initial exchanges between the first, second and super nodes in order to authenticate the first and second nodes to the super node, and further shifting energy usage to the super node by performing private key decryption at the super node, thus avoiding, at least in part, private key decryption at the first and second nodes;

~~whereby energy usage is shifted to the super node by performing private key decryption at the super node~~.

2. (Original) The method of claim 1, further comprising sending a second message from the first node to the second node, wherein the second message includes a first message authentication code.

3. (Original) The method of claim 2, further comprising authenticating the first partial key value at the second node using the first message authentication code.

4. (Original) The method of claim 1, further comprising:

sending a third message from the second node to the super node, wherein the third message includes the second partial key value encrypted using the public key belonging to the super node;

recovering the second partial key value at the super node by decrypting using the private key;

securely communicating the second partial key value to the first node; and

establishing the cryptographic key at the first node using the first partial key value and the second partial key value.

5. (Currently Amended) The method of claim 4, further comprising sending a fourth message from the second node to the first node, wherein the fourth message includes a second message authentication code.

6. (Original) The method of claim 5, further comprising authenticating the second partial key value at the first node using the second message authentication code.

7. (Original) The method of claim 4, wherein securely communicating the first partial key value to the second node includes:

encrypting the first partial key value at the super node using a second node symmetric key creating a first encrypted partial key value, wherein the second node symmetric key is received in the third message;

transmitting the first encrypted partial key value to the second node; and

decrypting the first encrypted partial key value at the second node to recover the first partial key value.

8. (Original) The method of claim 7, wherein the second node symmetric key is validated using a certificate provided by a recognized certificate authority and wherein the certificate is included in the third message.

9. (Original) The method of claim 8, wherein the certificate includes validation information for a plurality of symmetric keys and wherein a new second node symmetric key is selected periodically from the plurality of symmetric keys.

10. (Original) The method of claim 7, wherein the second node symmetric key is saved at the super node so that a subsequent key establishment can use symmetric key encryption for encrypting the first partial key value.

11. (Original) The method of claim 4, wherein securely communicating the second partial key value to the first node includes:

encrypting the second partial key value at the super node using a first node symmetric key creating a second encrypted partial key value, wherein the first node symmetric key is received in the first message and wherein the first node symmetric key is encrypted using the public key belonging to the super node;

transmitting the second encrypted partial key value to the first node; and

decrypting the second encrypted partial key value at the first node to recover the second partial key value.

12. (Original) The method of claim 11, wherein the first node symmetric key is validated using a certificate provided by a recognized certificate authority and wherein the certificate is included in the first message.

13. (Original) The method of claim 12, wherein the certificate includes validation information for a plurality of symmetric keys and wherein a new first node symmetric key is selected periodically from the plurality of symmetric keys.

14. (Original) The method of claim 11, wherein the first node symmetric key is saved at the super node so that a subsequent key establishment can use symmetric key encryption for encrypting the second partial key value.

15. (Original) The method of claim 4, wherein establishing the cryptographic key at the first node involves creating a hash of the first partial key value and the second partial key value.

16. (Original) The method of claim 4, wherein establishing the cryptographic key at the second node involves creating a hash of the first partial key value and the second partial key value.

17. (Original) The method of claim 4, further comprising establishing trust of the super node at the first node by validating a certificate provided by a recognized certificate authority and presented to the first node by the super node.

18. (Original) The method of claim 4, further comprising establishing trust of the super node at the second node by validating a certificate provided by a recognized certificate authority and presented to the second node by the super node.

19. (Currently Amended) A computer-readable storage medium storing instructions that when executed by a computer cause the computer to perform a method for establishing a cryptographic key for use between a first node and a second node using a super node, wherein the first node and the second node are energy-limited and the super node has abundant energy, the method comprising:

sending a first message from the first node to the super node, ~~wherein~~ the first message includesing a first partial key value encrypted using a public key belonging to the super node, ~~whereby~~the encrypting with the public key requiresing less energy than decrypting with a private key corresponding to the public key;

recovering the first partial key value at the super node by decrypting using the private key;

securely communicating the first partial key value to the second node; ~~and~~

establishing the cryptographic key at the second node using the first partial key value and a second partial key value created by the second node; and

utilizing a combination of public key cryptography and symmetric key cryptography with symmetric key encryption being used in initial exchanges between the first, second and super nodes in order to authenticate the first and second nodes to the super node, and further shifting energy usage to the super node by performing private key decryption at the super node, thus avoiding, at least in part, private key decryption at the first and second nodes;

~~whereby energy usage is shifted to the super node by performing private key decryption at the super node~~.

20. (Original) The computer-readable storage medium of claim 19, the method further comprising sending a second message from the first node to the

second node, wherein the second message includes a first message authentication code.

21. (Original) The computer-readable storage medium of claim 20, the method further comprising authenticating the first partial key value at the second node using the first message authentication code.

22. (Original) The computer-readable storage medium of claim 19, the method further comprising:

sending a third message from the second node to the super node, wherein the third message includes the second partial key value encrypted using the public key belonging to the super node;

recovering the second partial key value at the super node by decrypting using the private key;

securely communicating the second partial key value to the first node; and

establishing the cryptographic key at the first node using the first partial key value and the second partial key value.

23. (Original) The computer-readable storage medium of claim 22, the method further comprising sending a fourth message from the second node to the first node, wherein the fourth message includes a second message authentication code.

24. (Original) The computer-readable storage medium of claim 23, the method further comprising authenticating the second partial key value at the first node using the second message authentication code.

25. (Original) The computer-readable storage medium of claim 22, wherein securely communicating the first partial key value to the second node includes:

encrypting the first partial key value at the super node using a second node symmetric key creating a first encrypted partial key value, wherein the second node symmetric key is received in the third message;

transmitting the first encrypted partial key value to the second node; and

decrypting the first encrypted partial key value at the second node to recover the first partial key value.

26. (Original) The computer-readable storage medium of claim 25, wherein the second node symmetric key is validated using a certificate provided by a recognized certificate authority and wherein the certificate is included in the third message.

27. (Original) The computer-readable storage medium of claim 26, wherein the certificate includes validation information for a plurality of symmetric keys and wherein a new second node symmetric key is selected periodically from the plurality of symmetric keys.

28. (Original) The computer-readable storage medium of claim 25, wherein the second node symmetric key is saved at the super node so that a subsequent key establishment can use symmetric key encryption for encrypting the first partial key value.

29. (Original) The computer-readable storage medium of claim 22, wherein securely communicating the second partial key value to the first node includes:

encrypting the second partial key value at the super node using a first node symmetric key creating a second encrypted partial key value, wherein the first node symmetric key is received in the first message and wherein the first node symmetric key is encrypted using the public key belonging to the super node;

transmitting the second encrypted partial key value to the first node; and

decrypting the second encrypted partial key value at the first node to recover the second partial key value.

30. (Original) The computer-readable storage medium of claim 29, wherein the first node symmetric key is validated using a certificate provided by a recognized certificate authority and wherein the certificate is included in the first message.

31. (Original) The computer-readable storage medium of claim 30, wherein the certificate includes validation information for a plurality of symmetric keys and wherein a new first node symmetric key is selected periodically from the plurality of symmetric keys.

32. (Original) The computer-readable storage medium of claim 29, wherein the first node symmetric key is saved at the super node so that a subsequent key establishment can use symmetric key encryption for encrypting the second partial key value.

33. (Original) The computer-readable storage medium of claim 22, wherein establishing the cryptographic key at the first node involves creating a hash of the first partial key value and the second partial key value.

34. (Original) The computer-readable storage medium of claim 22, wherein establishing the cryptographic key at the second node involves creating a hash of the first partial key value and the second partial key value.

35. (Original) The computer-readable storage medium of claim 22, the method further comprising establishing trust of the super node at the first node by validating a certificate provided by a recognized certificate authority and presented to the first node by the super node.

36. (Original) The computer-readable storage medium of claim 22, the method further comprising establishing trust of the super node at the second node by validating a certificate provided by a recognized certificate authority and presented to the second node by the super node.

37. (Currently Amended) An apparatus that facilitates establishing a cryptographic key for use between a first node and a second node using a super node, wherein the first node and the second node are energy-limited and the super node has abundant energy, the apparatus comprising:

a first sending mechanism configured to send a first message from the first node to the second node, wherein the first message includes a first message authentication code;

the first sending mechanism further configured to send a second message from the first node to the super node, ~~wherein~~ the first message includes~~ing~~ a first partial key value encrypted using a public key belonging to the super node, ~~whereby~~the encrypting with the public key require~~s~~ing less energy than decrypting with a private key corresponding to the public key;

a decrypting mechanism configured to recover the first partial key value at the super node by decrypting using the private key;

a secure communication mechanism configured to securely communicate the first partial key value to the second node;

a first authenticating mechanism configured to authenticate the first partial key value at the second node using the first message authentication code; ~~and~~

a first establishing mechanism configured to establish the cryptographic key at the second node using the first partial key value and a second partial key value created by the second node; and

means for utilizing a combination of public key cryptography and symmetric key cryptography with symmetric key encryption being used in initial exchanges between the first, second and super nodes in order to authenticate the first and second nodes to the super node, and further shifting energy usage to the super node by performing private key decryption at the super node, thus avoiding, at least in part, private key decryption at the first and second nodes;

~~whereby energy usage is shifted to the super node by performing private key decryption at the super node~~.

38. (Original) The apparatus of claim 37, further comprising:

a second sending mechanism configured to send a third message from the second node to the first node, wherein the third message includes a second message authentication code;

the second sending mechanism further configured to send a fourth message from the second node to the super node, wherein the fourth message includes the second partial key value encrypted using the public key belonging to the super node;

the decrypting mechanism further configured to recover the second partial key value at the super node by decrypting using the private key;

the secure communication mechanism further configured to securely communicating the second partial key value to the first node;

a second authenticating mechanism configured to authenticate the second partial key value at the first node using the second message authentication code; and

a second establishing mechanism configured to establish the cryptographic key at the first node using the first partial key value and the second partial key value.

39. (New) A method for establishing a cryptographic key for use between a first node and a second node using a super node, wherein the first node and the second node are energy-limited and the super node has abundant energy, the method comprising:

sending a first message from the first node to the super node, the first message including a first partial key value encrypted using a public key belonging to the super node, the encrypting with the public key requiring less energy than decrypting with a private key corresponding to the public key;

recovering the first partial key value at the super node by decrypting using the private key;

securely communicating the first partial key value to the second node;

establishing the cryptographic key at the second node using the first partial key value and a second partial key value created by the second node; and

utilizing a combination of public key cryptography and symmetric key cryptography with symmetric key encryption being used in initial exchanges between the first, second and super nodes in order to authenticate the first and second nodes to the super node, and further shifting energy usage to the super node by performing private key decryption at the super node, thus avoiding, at least in part, private key decryption at the first and second nodes;

wherein a second message is sent from the first node to the second node, wherein the second message includes a first message authentication code;

wherein the first partial key value is authenticated at the second node using the first message authentication code;

wherein the method further comprises:

sending a third message from the second node to the super node, wherein the third message includes the second partial key value encrypted using the public key belonging to the super node;

recovering the second partial key value at the super node by decrypting using the private key;

securely communicating the second partial key value to the first node; and

establishing the cryptographic key at the first node using the first partial key value and the second partial key value;

wherein a fourth message is sent from the second node to the first node, wherein the fourth message includes a second message authentication code;

wherein the second partial key value is authenticated at the first node using the second message authentication code;

wherein securely communicating the first partial key value to the second node includes:

encrypting the first partial key value at the super node using a second node symmetric key creating a first encrypted partial key value, wherein the second node symmetric key is received in the third message;

transmitting the first encrypted partial key value to the second node; and

decrypting the first encrypted partial key value at the second node to recover the first partial key value;

wherein the second node symmetric key is validated using a certificate provided by a recognized certificate authority and wherein the certificate is included in the third message;

wherein the certificate includes validation information for a plurality of symmetric keys and wherein a new second node symmetric key is selected periodically from the plurality of symmetric keys;

wherein the second node symmetric key is saved at the super node so that a subsequent key establishment can use symmetric key encryption for encrypting the first partial key value;

wherein securely communicating the second partial key value to the first node includes:

encrypting the second partial key value at the super node using a first node symmetric key creating a second encrypted partial key value, wherein the first node symmetric key is received in the first message and wherein the first node symmetric key is encrypted using the public key belonging to the super node;

transmitting the second encrypted partial key value to the first node; and

decrypting the second encrypted partial key value at the first node to recover the second partial key value;

wherein the first node symmetric key is validated using a certificate provided by a recognized certificate authority and wherein the certificate is included in the first message;

wherein the certificate includes validation information for a plurality of symmetric keys and wherein a new first node symmetric key is selected periodically from the plurality of symmetric keys;

wherein the first node symmetric key is saved at the super node so that a subsequent key establishment can use symmetric key encryption for encrypting the second partial key value;

wherein establishing the cryptographic key at the first node involves creating a hash of the first partial key value and the second partial key value;

wherein establishing the cryptographic key at the second node involves creating a hash of the first partial key value and the second partial key value;

wherein trust of the super node is established at the first node by validating a certificate provided by a recognized certificate authority and presented to the first node by the super node;

wherein trust of the super node is established at the second node by validating a certificate provided by a recognized certificate authority and presented to the second node by the super node.